Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651 -00xx
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| | | |
|---|---|---|
| **PRE-APPEAL BRIEF REQUEST FOR REVIEW** | Docket Number (Optional)<br>PR 1803.01 US | |
| I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to **"Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450"** [37 CFR 1.8(a)]<br>on 9.28.2007<br>Signature<br>Typed or printed name Bac-Ha Phan | Application Number<br>10/605,173 | Filed<br>09/12/2003 |
| | First Named Inventor<br>Ashot Andreasyan | |
| | Art Unit<br>2135 | Examiner<br>HA, Leynna A. |

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 47,529

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 ______

Signature

Caroline T. Do, Reg. No. 47,529
Typed or printed name

(310) 952-3312
Telephone number

09/28/07
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 *and select* option 2.

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Ashot Andreasyan

Application No.: 10/605,173

Filed: September 12, 2003

For: KEY EXCHANGE BASED ON DSA TYPE CERTIFICATES

Examiner: Leynna A. Ha

Art Unit: 2135

Confirmation No.: 2172

Docket No.: PR 1803.01 US

## PRE-APPEAL BRIEF REQUEST FOR REVIEW

**Mail Stop AF**
Commissioner for Patents
PO Box 1450
Alexandria VA 22313-1450

**CERTIFICATE OF ELECTRONIC TRANSMISSION**

I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office on:

9. 28. 2007 Bac-Ha Phan
(Date) (Type or Print Name)

(Signature)

Sir:

In response to the Final Office action dated July 2, 2007, Applicant would like to request a pre-appeal panel review of the application.

**Remarks/Arguments** begin on page 2 of this paper.

**REMARKS/ARGUMENTS**

Claims 1-35 are pending in the present application.

This Request is in response to the Final Office Action mailed July 2, 2007. In the Office Action, the Examiner rejected: 1) claims 1-32 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,677,888 issued to Roy (hereinafter "Roy") and 2) claims 33-35 under 35 U.S.C. §103(a) as being unpatentable over Roy, and further in view of U.S Patent No. 7,222,187 issued to Yeager (hereinafter "Yeager"). For the purpose of the Pre-Appeal Brief Request for Review, Applicant would make remarks/arguments in response to the 35 U.S.C. §102(e) rejection to independent claims 1, 9, 17, and 25 only. More details of Applicants remarks/arguments will be presented in the Appeal Brief at a latter time. Reconsideration in light of the remarks made herein is respectfully requested. Applicant respectfully traverses the rejections and contends that the Examiner has not established a prima facie case of anticipation.

Pre-appeal panel review of the application in light of the remarks/arguments made herein is respectfully requested.

There are several clear errors in the Examiner's rejections and arguments.

1) Roy does not disclose *the step of "performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters", the Examiner cited Roy (col. 9, lines 44-60). The Examiner stated, "Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1st parameters being signature standard parameters." There is nothing in Roy that discloses using a DSS parameter to generate a public key. Roy only discloses, "… To sign a message M, the SAM processes M with a known hash function called SHA-1, thereby obtaining a digital fingerprint SHA-1(M) of the message …" Roy discloses*

*the generating of ECC certificate when the present invention assumes that the certificate has already issued by CA.*

2) Roy does not disclose *the step of "providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters", the Examiner cited* Roy *(col. 10, lines 27-32). The Examiner stated, "Roy discloses the CA issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2nd certificate and public key with 2nd parameters." This may be true. Each system can choose to use some CA and key sizes can be defined as well. However, defining and enrolling certificates are out of the scope of the claimed invention. As stated before, the claimed invention assumes that certificates are already issued by CA and both peers have DSA type of certificates and that they are valid. Furthermore, the first public key provided from the second peer to the first peer was calculated using a DSS parameter. There in nothing in* Roy *that discloses the public key was generated using a DSS parameter.*

3) Roy does not disclose *the step of "performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters", the Examiner cited* Roy *(col. 10, lines 48-52). The Examiner stated, "Roy discusses a secret session key is established in a request message that sends the message with the signature as the claimed shared secret key using a parameter from the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above."* Roy *discloses protocol between aircraft and ground SAM. The present invention is not a protocol. It is a key exchange method, key establishment method, which can be used in any protocol as well as the protocol disclosed in* Roy.

4) Roy does not disclose *the step of "performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer", the Examiner cited* Roy *(col. 10, lines 1-9).* Roy *discloses an elliptic curve Diffie-Hellman key agreement*

*scheme that operates as follows: when two entities (U and V) want to establish a shared secret key, they exchange their public keys $d_uG$ and $d_VG$ where $d_u$ and $d_v$ are private keys of the corresponding entities U and V. Then both entities compute a share secret ... Roy discloses how Diffie-Hellman shared secret is established on ECC. The mechanism in the claimed invention is different. First of all, it uses DSA parameters, which are not the same as DH parameters. Secondly, the first peer in the claimed invention does not generate DH public/private key. It just sends its certificate. The second peer in the claimed invention generates public/private key pair by using DSA parameters from the certificate sent from the first peer. Furthermore, classic DH key exchange (which is disclosed in Roy) requires 4 exponentiation operations (2 on each side). Each side uses 2 exponentiation operations; one for generating DH public/private key and one for generating shared secret key. The claimed invention can generate a shared secret key by a total of 3 exponentiation operations only.*

Accordingly, Applicant respectfully requests the Review Panel render a decision allowing the application.

**CONCLUSION**

Applicant respectfully requests the Review Panel render a decision allowing the application.

Respectfully submitted,

DISCOVISION ASSOCIATES

Dated: 09/28/07

By:____________________
Caroline T. Do
Reg. 47,529
Tel.: (310) 952-3312 (Pacific Coast)

DISCOVISION ASSOCIATES
INTELLECTUAL PROPERTY DEVELOPMENT
2265 E. 220th Street
Long Beach, CA 90810
(310) 952-3300

P:\ABG\PPD\PR\1803\01\PreAppeal_Req Review_01.doc